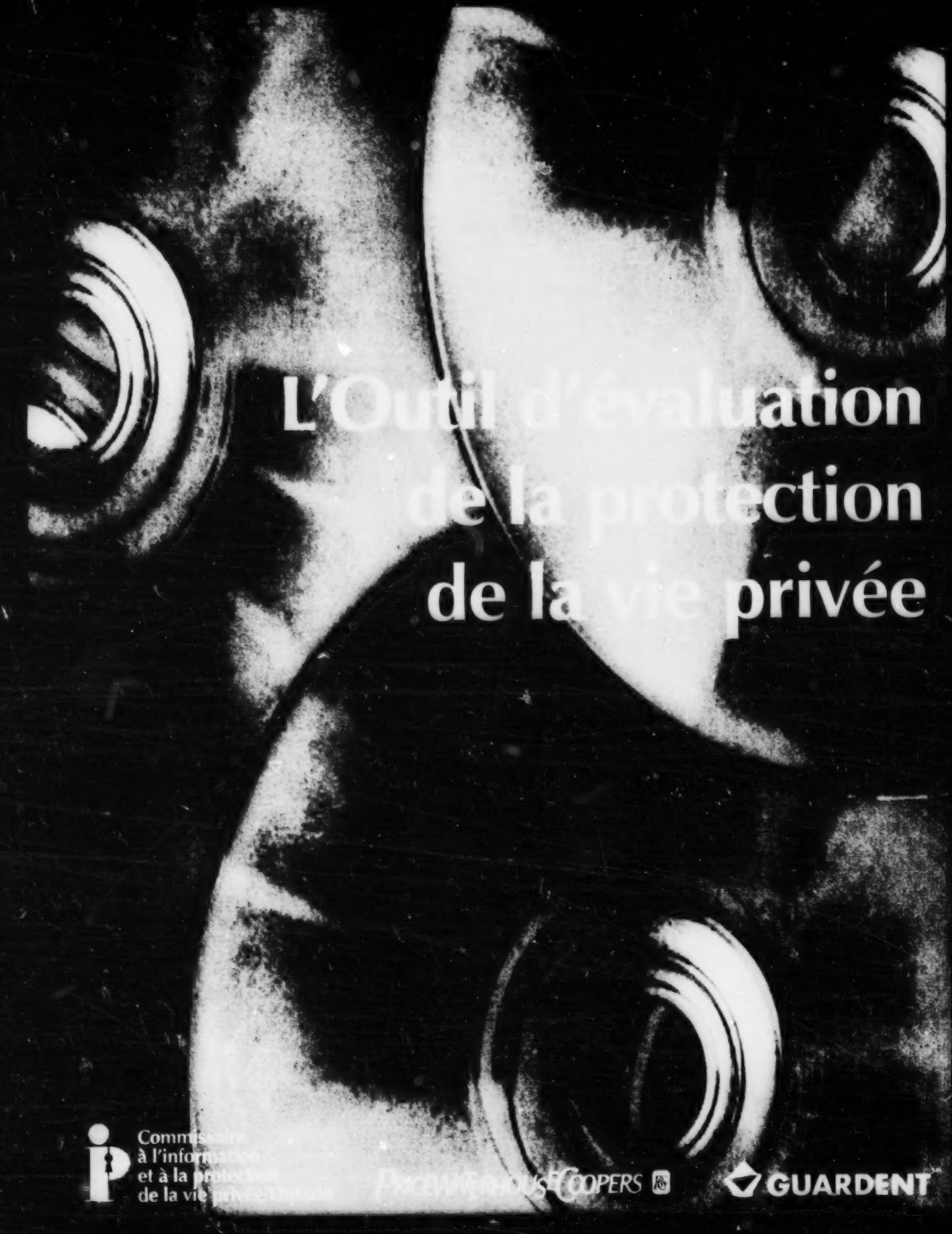

L'Outil d'évaluation de la protection de la vie privée

Commissariat à l'information et à la protection de la vie privée

Price Waterhouse Coopers

GUARDENT

L'Outil d'évaluation de la protection de la vie privée est disponible sur le site Web du Bureau du commissaire à l'information et à la protection de la vie privée/Ontario.

This publication is also available in English.

Commissaire à l'information et à la protection de la vie privée/Ontario
80, rue Bloor ouest, Bureau 1700
Toronto (Ontario) M5S 2V1
416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

GUARDENT℠

GUARDENT Inc.
75 Third Avenue
Waltham, MA 02451
781-577-6500
Fax: 781-577-6600
Web site: www.guardent.com

PRICEWATERHOUSECOOPERS

PricewaterhouseCoopers
Global Risk Management Solutions
145, rue King Ouest
Toronto (Ontario) M5H 1V8
416-814-5729
Télécopieur : 416-814-5777
Courriel : michael.deck@ca.pwcglobal.com

Avant-propos

Il ne fait aucun doute qu'un nombre croissant d'entreprises veulent en apprendre davantage sur la protection de la vie privée et sur la façon de protéger les renseignements personnels de leurs clients. C'est ce que des enquêtes ont démontré. Par ailleurs, le fait que mon bureau reçoit de plus en plus de demandes d'allocutions en provenance du secteur privé vient directement appuyer une telle constatation. Au cours de l'année précédente, plus particulièrement, j'ai remarqué qu'après chacune de mes allocutions ou présentations, les gens d'affaires venaient me voir pour me demander : *Par où dois-je commencer? Quelle est la première étape pour protéger les renseignements de mes clients?* et *Quels sont les outils disponibles qui pourraient m'aider?* Malheureusement, je n'avais à peu près pas de ressources à leur conseiller et fort peu d'outils utiles à leur offrir.

Aux prises avec cette déconvenue, j'ai soudain réalisé qu'il fallait un outil simple basé sur des questions et des réponses à l'intention des entreprises qui cherchaient de l'assistance et des conseils pour assurer la confidentialité de façon concrète. Ces entreprises ont besoin d'aide, non seulement afin de déterminer si elles sont prêtes à assurer la protection de la vie privée mais aussi pour connaître quelles sont les étapes à franchir pour relever les lacunes et y remédier.

Cette situation m'a incitée à faire deux choses : premièrement, j'ai essayé de combler le manque en mettant au point une certaine forme d'outil de diagnostic relatif à la protection des renseignements personnels et, deuxièmement, j'ai cherché de l'aide auprès de personnes connaissant bien le milieu des affaires afin de m'assurer que l'outil serait à la fois pertinent et adapté aux besoins. J'ai sollicité Guardent et PricewaterhouseCoopers afin qu'ils collaborent à un projet avec mon bureau. À ma plus grande joie, tous les deux ont gracieusement accepté de travailler avec nous afin de mettre au point l'Outil d'évaluation de la protection de la vie privée que vous avez en main. Leur expertise dans le domaine des affaires a été précieuse; associée à notre propre expertise en matière de protection des renseignements personnels, elle a mené à la création de ce nouvel outil convivial destiné aux entreprises.

J'aimerais remercier sincèrement Guardent et PricewaterhouseCoopers d'avoir travaillé avec nous afin de concevoir ce que je considère être un excellent outil.

J'aimerais aussi remercier le Centre francophone d'informatisation des organisations (CEFRIO) d'avoir collaboré à la production de la version française de ce document. Dans les divers projets de recherche-action qu'il mène avec ses partenaires des secteurs public et privé, le CEFRIO a relevé l'importance que revêtent inévitablement les questions de confidentialité pour le citoyen ou pour le consommateur. Je suis fière qu'avec son aide, l'Outil d'évaluation de la protection de la vie privée est maintenant à la portée de l'ensemble des entreprises francophones du Canada.

Je suis certaine que vous trouverez cet outil très utile lorsque vous ferez face aux défis d'assurer la protection de la vie privée dans une économie en constant changement axée sur la collecte de renseignements. Je vous souhaite le plus grand succès.

Ann Cavoukian, Ph.D.
Commissaire

Table des matières

Introduction 1

Principe 1 — La responsabilité 5

Principe 2 — La détermination des fins de la collecte des renseignements 8

Principe 3 — Le consentement 11

Principe 4 — La limitation de la collecte 14

Principe 5 — La limitation de l'utilisation, de la communication et de la conservation .. 17

Principe 6 — L'exactitude 21

Principe 7 — Les mesures de sécurité 23

Principe 8 — La transparence 27

Principe 9 — L'accès aux renseignements personnels 30

Principe 10 — Plainte contre le non-respect des principes 33

Glossaire des termes 35

Liens vers d'autres sites sur la confidentialité 39

Introduction

En janvier 2000, le *Wall Street Journal* publiait une enquête selon laquelle la protection des renseignements personnels constituait la première préoccupation des Nord-Américains pour le 21e siècle. Plus récemment, le 5 mars 2001, Forrester Research déposait une étude sur les enjeux relatifs à la protection de la vie privée pour les entreprises. On y faisait la déclaration suivante : « Toute personne, aujourd'hui, qui croit que la question de la protection de la vie privée a atteint son paroxysme se trompe grandement ... nous sommes au tout début d'un changement majeur sur le plan des attitudes, lequel alimentera des batailles politiques et enverra sous le microscope des pratiques commerciales qui étaient courantes. »

En même temps, les progrès réalisés en technologie de l'information et Internet ont changé la façon dont les entreprises font des affaires. Au cours des dix dernières années, nous avons assisté à une avancée sans précédent en ce qui concerne la capacité des organisations à recueillir, compiler, analyser et diffuser des renseignements personnels qui sont amassés de façon courante. Comme le *Wall Street Journal*, entre autres, le démontre, les consommateurs s'attendent à ce que leurs renseignements personnels soient protégés et que leur vie privée soit respectée par les organisations avec lesquelles ils font affaire. En trahissant les attentes du consommateur, les organisations se positionnent du mauvais côté dans l'enjeu sur la protection de la vie privée.

Aujourd'hui, les entreprises chefs de file reconnaissent que les questions de confidentialité menacent les fondements. De plus, on commence à réaliser que s'attaquer efficacement aux problèmes de la protection des renseignements personnels constitue une stratégie gagnante autant pour l'entreprise que pour les consommateurs.

Qu'est-ce que la protection de la vie privée et pourquoi est-ce important?

Une grande variété de valeurs, de droits et d'intérêts interreliés sont regroupés sous la rubrique « protection de la vie privée ». Cependant, pour la plupart des entreprises sa sous-catégorie la plus pertinente est la protection des renseignements (aussi appelée protection des données).

La protection des renseignements est la capacité qu'a chacun d'exercer un degré de contrôle important sur la collecte, l'utilisation et la divulgation de ses renseignements personnels.

Les renseignements personnels comprennent toute information sur une personne identifiable dont le nom, l'adresse, le sexe, l'âge, les numéros d'identification, le revenu, l'origine ethnique, les dossiers de l'employé, le dossier de crédit ou le dossier médical. Il n'est pas nécessaire que le nom de la personne soit attaché à l'information pour qu'elle soit qualifiée de renseignement personnel.

La plupart des entreprises ont besoin de recueillir, d'utiliser et de divulguer de l'information au sujet de leurs clients dans la conduite de leurs affaires. Mais les organisations doivent être raisonnables et justes dans leur façon de traiter les renseignements personnels, non seulement pour le bien de leurs clients mais également pour celui de la réputation de leur propre entreprise. Les consommateurs ne sont plus prêts à fermer les yeux lorsqu'une entreprise ne protège pas leur vie privée. Des mauvais usages de renseignements personnels qui

ont été fortement médiatisés ont démontré qu'un manque de respect envers la vie privée peut entraîner aussi bien des critiques sévères des consommateurs qu'une dévaluation importante des actions d'une entreprise.

Grâce, en partie, à des incidents qui ont fait la manchette, de nombreuses collectivités publiques ont connu une vague d'initiatives législatives telles que la *directive de l'Union européenne sur la protection des données* et la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada. Les organisations de partout dans le monde commencent à remarquer les initiatives de réglementation internationales et locales qui pourraient influencer la façon dont elles traitent l'information relative aux clients.

Le moment est propice pour les organisations qui gèrent des renseignements personnels d'examiner leurs pratiques de près et de les harmoniser avec les nouvelles attentes des consommateurs. À court terme, le fait de protéger les renseignements personnels et de gagner la confiance du consommateur deviendra assurément un avantage concurrentiel important. À long terme, la protection de la vie privée deviendra un nouvel impératif en affaires.

L'Outil d'évaluation de la protection de la vie privée : en quoi peut-il m'être utile?

Les organisations qui souhaitent faire des affaires doivent prendre la question de la protection de la vie privée très au sérieux. Selon un groupe de cadres supérieurs qui ont pris part à la *Computerworld* Premier 100 Conference en mai 2001, même un simple écart en matière de confidentialité pourrait avoir des effets dévastateurs sur l'image corporative et la marque d'une entreprise.

Est-ce que le fait de s'intéresser à l'Outil d'évaluation de la protection de la vie privée et de prendre le temps de l'utiliser peut profiter à une organisation? Afin de vous aider, vous et votre organisation, à décider d'utiliser ou non cet outil, nous vous recommandons de lire les questions suivantes. Si votre organisation répond par l'affirmative à au moins une des questions, vous tirerez des avantages à utiliser l'Outil d'évaluation de la protection de la vie privée. En fait, nous le recommandons vivement.

Questions

1. Est-ce que votre organisation recueille et utilise des renseignements personnels dans le cadre des activités de votre entreprise?

2. L'utilisation de renseignements personnels constitue-t-elle une partie importante de votre entreprise (par exemple, dans le cadre de la mise en marché, des ventes ou de la gestion des relations clients)?

3. Est-ce que vous communiquez des renseignements sur vos clients à quiconque?

4. Avez-vous acheté, vendu, échangé ou communiqué des renseignements personnels?

5. Votre organisation est-elle potentiellement vulnérable à des brèches de sécurité internes ou externes qui concernent les renseignements personnels de vos clients?

6. Vous posez-vous des questions sur l'incidence que les règlements actuels et futurs en matière de protection de la vie privée auront sur votre façon de recueillir et d'utiliser les renseignements personnels?

Si vous avez répondu oui à au moins une des questions ci-dessus, vous aurez avantage à utiliser l'Outil d'évaluation de la protection de la vie privée.

L'utilisation de l'Outil d'évaluation de la protection de la vie privée

L'outil vous permet d'évaluer vous-même, sur une base volontaire, si les méthodes de gestion des renseignements de votre entreprise respectent la vie privée de vos clients et dans quelle mesure. Par le biais d'une série de questions, l'outil d'évaluation vous aidera autant à évaluer votre organisation qu'à lui fournir de l'information pertinente; ainsi, vous comprendrez mieux comment protéger les renseignements personnels et gagner la confiance du consommateur.

L'Outil d'évaluation de la protection de la vie privée porte sur dix principes qui sont essentiels à la bonne gestion des renseignements personnels; ils sont basés sur les pratiques équitables de traitement de l'information, des normes reconnues au niveau international. Ces pratiques équitables sont des principes cumulatifs qui se chevauchent. Ils exposent les méthodes responsables de traitement de l'information et couvrent les domaines suivants :

- La responsabilité
- La définition des objectifs
- Le consentement
- La limitation de la collecte
- La limitation de l'utilisation, de la divulgation et de la durée de conservation des renseignements personnels
- L'exactitude des renseignements
- Les mesures de sécurité
- La transparence
- L'accès des particuliers
- La possibilité de porter plainte contre le non-respect des principes

L'Outil d'évaluation de la protection de la vie privée décrit chaque principe, en explique les objectifs et signale certains risques auxquels votre entreprise peut faire face si elle n'y adhère pas.

Pour chaque principe, il y a une série de questions sur la mise en application qui sont divisées en deux sections. La première section, *Mise en application des principes*, établit et évalue votre degré de conformité avec les étapes *requises* dans la mise en application du principe. La seconde section, *Pratiques exemplaires*, établit et évalue votre degré de conformité avec les *pratiques exemplaires* dans la mise en application du principe. Répondez simplement par *Oui* ou *Non* à chaque question selon les pratiques courantes de votre entreprise. Si l'exigence ou la pratique exemplaire n'est pas pertinente pour votre organisation, répondez *Oui*.

Si vous avez répondu *Non* à l'une des questions sous la rubrique *Ce que vous devez faire*, votre organisation n'adhère pas complètement à cette pratique équitable de traitement de l'information. Vous devriez examiner et modifier vos politiques et procédures afin de pouvoir répondre par l'affirmative. Si vous avez répondu *Non* à l'une des *pratiques exemplaires*, demandez-vous si vous devriez adopter cette pratique au sein de votre organisation.

À propos de l'Outil d'évaluation de la protection de la vie privée

Veuillez prendre note que cet outil n'a pas été conçu dans le but de fournir une évaluation détaillée ni une analyse d'impact approfondie en matière de protection des renseignements personnels. On devrait utiliser cet outil pour obtenir une évaluation initiale de sa conformité aux principes relatifs à la protection de la vie privée. Il se veut un complément aux autres mesures que vous pourriez adopter pour protéger la vie privée de vos clients et à toutes autres mesures que vous pourriez devoir prendre afin de vous conformer à la législation relative à la confidentialité des renseignements personnels et aux autres normes juridiques ou codes de la confidentialité du secteur d'activités s'appliquant à votre organisation.

Nous nous sommes efforcés de créer un outil qui soit le plus efficace possible. Cependant, le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario (CIPVP) n'assume aucune responsabilité légale quant aux résultats liés à l'utilisation de cet outil. L'information contenue dans cette publication ne devrait pas être considérée comme une consultation ou un service d'un spécialiste en matière de loi, de comptabilité, de fiscalité ou de tout autre professionnel. (Si vous avez besoin d'un conseil particulier relativement à une situation précise, vous devriez toujours consulter un spécialiste ayant les qualifications requises.)

L'Outil d'évaluation de la protection de la vie privée a été conçu par le CIPVP avec la généreuse assistance de Guardent et PricewaterhouseCoopers et, pour sa version française, du CEFRIO. Toute erreur ou omission sont l'entière responsabilité du CIPVP.

L'Outil d'évaluation de la protection de la vie privée est offert gratuitement à toute entreprise désirant faire l'examen de ses politiques de gestion de l'information ou aux consommateurs qui voudraient un outil afin d'analyser les méthodes en matière de confidentialité des entreprises avec lesquelles ils entretiennent des liens. Le questionnaire est aussi conçu dans le but d'être rempli dans l'anonymat et n'exige pas de la part de l'utilisateur de fournir des résultats ou de l'information aux concepteurs.

Principe 1 La responsabilité

Une organisation est responsable des renseignements personnels qui sont sous son contrôle et désignera une ou des personnes qui devront s'assurer qu'elle respecte les principes énoncés en matière de protection de la vie privée.

Objectifs

Ce principe vise à déterminer la responsabilité ultime en termes de conformité. La responsabilisation garantira une mise en application, une élaboration de politiques, une observation, une évaluation et un perfectionnement efficaces en matière de protection de la vie privée dans l'ensemble de votre organisation.

Vous devez appliquer vos politiques et pratiques en matière de confidentialité à **tous** les renseignements personnels qui sont sous votre contrôle. L'information sous votre contrôle englobe non seulement les données que vous conservez mais également les renseignements personnels que vous pouvez avoir transférés à un tiers, comme à un contractant, pour le traitement des données.

Risque potentiel

- Une responsabilité mal définie pourrait entraîner la mauvaise gestion de l'information sur le client (par ex. trahir la confiance du client, divulguer de façon inappropriée des renseignements personnels) et, de là, nuire à votre réputation et à vos relations d'affaires.

- Une responsabilité mal définie fera en sorte qu'il vous sera plus difficile de donner suite aux plaintes des clients de manière efficace, ce qui entraînera une insatisfaction chez le client et la perte potentielle de contrats.

- Une responsabilité mal définie vous nuira lorsque vous tenterez d'obtenir une analyse valable des pratiques de gestion de l'information de votre entreprise.

Mise en application du principe

Ce que vous devez faire

- Vous conférez la responsabilité de veiller au respect de ces principes à une personne ou à un groupe de personnes précis de votre entreprise.

☐ Oui ☐ Non

- Vous communiquez l'identité et les coordonnées de la personne ou du groupe de personnes de votre organisation qui sont responsables de veiller au respect des principes énoncés en matière de confidentialité.

☐ Oui ☐ Non

- Vous élaborez puis mettez en application des politiques et procédures précis en matière de protection de la vie privée.

☐ Oui ☐ Non

- Vous utilisez des contrats et (ou) d'autres mesures afin de vous assurer, lorsqu'un tiers traite les renseignements personnels pour votre compte, que ses pratiques de protection de la confidentialité sont comparables aux vôtres.

☐ Oui ☐ Non

- Vous avez mis sur pied une procédure de gestion des plaintes afin de recevoir les plaintes et les requêtes relatives à vos pratiques de gestion de l'information et d'y donner suite.

☐ Oui ☐ Non

- Vous formez votre personnel et veillez à ce qu'il comprenne vos politiques et pratiques relatives à la confidentialité et qu'il puisse les mettre en application.

☐ Oui ☐ Non

Pratiques exemplaires

- Vous révisez régulièrement vos politiques et pratiques en matière de protection de la vie privée avec le personnel afin d'assurer une mise en application cohérente.

  ☐ Oui ☐ Non

- Vous avez une politique écrite en vigueur qui définit votre responsabilité relative aux renseignements personnels.

  ☐ Oui ☐ Non

- Le personnel de première ligne est formé pour gérer les requêtes des clients en matière de :
  - plaintes relatives à la confidentialité;
  - demandes de rectification; et
  - demandes d'accès à leurs renseignements personnels.

  ☐ Oui ☐ Non

- Vous avez instauré un système de surveillance continu de la conformité.

  ☐ Oui ☐ Non

- Vous avez intégré vos politiques et pratiques de gestion de l'information à la formation des nouveaux employés.

  ☐ Oui ☐ Non

- Vous définissez clairement les responsabilités de chaque employé et les révisez régulièrement.

  ☐ Oui ☐ Non

- Vous avez des vérifications et des mécanismes d'exécution précis (ex. des contrats) afin de veiller à ce que les tiers recueillent, utilisent et divulguent les renseignements personnels de manière appropriée.

  ☐ Oui ☐ Non

- Le respect efficace des principes de confidentialité fait partie de l'évaluation du rendement des personnes qui ont été désignées responsables des politiques de protection de la vie privée au sein de l'organisation.

  ☐ Oui ☐ Non

Principe 2 La détermination des fins de la collecte des renseignements

Avant ou au moment où l'information est recueillie, l'organisation doit déterminer à quoi serviront les renseignements personnels.

Objectifs

Déterminer à quelles fins vous avez besoin de renseignements personnels pour la conduite de vos affaires constitue une étape essentielle dans le but de définir la nature de l'information que vous devez recueillir, utiliser et divulguer. Vos objectifs devraient être raisonnables dans le contexte de votre entreprise. De plus, vous devez vous assurer qu'ils ne sont pas trop vagues pour que la personne de qui vous désirez obtenir des renseignements personnels puissent en saisir le sens.

Lorsque vous définissez vos objectifs, tenez compte des actions suivantes :

- **collecte** – quels renseignements personnels vous recueillez ou obtenez de quelque source que ce soit, y compris des tiers, par quels moyens et pour quelles raisons;
- **utilisation** – comment vous gérez et utilisez les renseignements personnels dans votre entreprise; et
- **divulgation** – quand, comment et pourquoi vous permettez à des tiers qui ne font pas partie de votre entreprise d'avoir accès à des renseignements personnels.

Risque potentiel

- Le fait de recueillir plus de renseignements que nécessaire peut exposer votre organisation à de plus grands risques en matière de responsabilité et de sécurité.
- À défaut de concevoir des processus adaptés au besoin de l'entreprise, de l'information non voulue pourrait être recueillie par inadvertance et occasionner des frais d'administration additionnels.
- Le fait de ne pas informer les clients sur le motif de la collecte de renseignements personnels peut vous faire perdre des clients.
- Il vous sera difficile de gérer de façon responsable l'information dont vous assurez la garde si vous ne définissez pas les motifs de la collecte de renseignements personnels.

Mise en application du principe

Ce que vous devez faire

- Vous déterminez les objectifs légitimes de la collecte de renseignements personnels avant ou au moment de recueillir l'information.

  ☐ Oui ☐ Non

- Vous déterminez quels renseignements sont nécessaires pour répondre aux objectifs fixés en tenant compte à la fois des objectifs principaux et secondaires (ex. vérification, marketing, etc.).

  ☐ Oui ☐ Non

- Vous détaillez vos objectifs afin que votre personnel et les personnes en lien avec l'information les comprennent.

  ☐ Oui ☐ Non

- Lorsque vous voulez utiliser des renseignements personnels déjà sous votre garde dans un but nouveau qui **n'avait pas** été fixé au moment de la collecte initiale, vous demandez l'autorisation de la personne concernée, à moins que le but nouveau ne soit une exigence de la loi.

  ☐ Oui ☐ Non

- Vous avez examiné, dans le but d'atteindre vos objectifs, les possibilités qui existaient d'utiliser des renseignements non identifiables (par ex. des renseignements codés, anonymes, des pseudonymes ou des données cumulatives) plutôt que des renseignements personnels.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Les objectifs de la collecte de renseignements personnels que vous vous êtes fixés sont accessibles au public au moment de la collecte.

  ☐ Oui ☐ Non

- Les employés qui recueillent les renseignements personnels peuvent expliquer aux particuliers les raisons pour lesquelles l'information est amassée.

  ☐ Oui ☐ Non

- Vous avez mis en place des procédures claires pour demander le consentement éclairé d'un client avant d'utiliser ou de divulguer des renseignements personnels à des fins autres que celles qui avaient été exprimées au moment de la collecte.

  ☐ Oui ☐ Non

- Vous réévaluez régulièrement les objectifs de la collecte de renseignements personnels afin de veiller à ce qu'ils restent à jour.

  ☐ Oui ☐ Non

- Les objectifs de la collecte des renseignements personnels qui ont été fixés sont transmis aux secteurs de l'entreprise responsables du traitement et de la collecte des données.

  ☐ Oui ☐ Non

- Le personnel est proactif et explique aux clients quels renseignements personnels sont recueillis et dans quel but.

  ☐ Oui ☐ Non

Principe 3 Le consentement

On doit informer toute personne et obtenir son consentement éclairé si l'on veut recueillir, utiliser ou divulguer des renseignements qui la concernent, à moins que la loi ne prévoie une exception.

Objectifs

Ce principe vous met dans l'obligation formelle d'obtenir le consentement des personnes dans le but de recueillir, d'utiliser et de divulguer leurs données, sauf dans certains cas.

Ce principe exige deux choses; que la personne soit informée et donne son consentement. Ainsi, vous ne devriez pas demander un consentement à moins que vous n'ayez fait un effort raisonnable d'informer les personnes sur les motifs de la collecte, de l'utilisation et de la divulgation de leurs renseignements personnels. De plus, vous ne devriez pas utiliser le consentement pour tenter de vous soustraire à vos obligations et responsabilités liées à ces principes.

Le consentement est un accord délibéré avec ce qui est fait ou proposé. On peut obtenir un consentement d'une variété de façons; il peut être explicite ou tacite. Vous devriez évaluer la sensibilité des renseignements personnels en jeu lorsque vous déterminez quelle méthode conviendra. Règle générale, plus les dommages que les personnes risquent d'encourir sont graves si leurs renseignements personnels sont mal utilisés, plus grande est votre responsabilité de veiller à ce que leur consentement soit éclairé et explicite.

Risque potentiel

- Le fait de ne pas demander le consentement ou de le demander de façons qui ne sont pas appropriées à la sensibilité de l'information pourrait miner la confiance du client et entraîner une réaction indésirable ce qui, en retour, pourrait ternir la réputation de l'entreprise.
- Le fait de ne pas obtenir le consentement peut diminuer l'efficacité de certaines pratiques commerciales, comme le marketing, en offrant par exemple des produits et services à une clientèle mal ciblée.
- Le fait de ne pas obtenir de consentement entraînera des obligations ou des sanctions légales lorsque, selon la loi, il est obligatoire de le demander.
- Le fait de ne pas obtenir de consentement formel peut inciter les clients à refuser de le donner plus tard pour l'utilisation de l'information.

Mise en application du principe

Ce que vous devez faire

- Vous obtenez le consentement pour recueillir, utiliser et divulguer les renseignements personnels avant ou au moment de la collecte, sauf lorsque cela n'est pas approprié (ex. échange d'information avec une agence de crédit pour l'octroi d'un prêt).

  ☐ Oui ☐ Non

- Vous tenez compte de la sensibilité des renseignements personnels lorsque vous déterminez quel type de consentement convient à la situation (par ex. consentement explicite ou tacite; accord ou désaccord).

  ☐ Oui ☐ Non

- Vous faites un effort raisonnable d'informer la personne à quelles fins l'information sera utilisée.

  ☐ Oui ☐ Non

- Lorsque vous cherchez à obtenir le consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels pour des motifs secondaires (comme le marketing), vous ne devez pas imposer de conditions comme refuser de fournir vos produits ou services si l'accord n'est pas consenti.

  ☐ Oui ☐ Non

- Vous ne trompez ni ne dupez la personne afin d'obtenir son consentement.

  ☐ Oui ☐ Non

- Vous informez les gens du fait qu'ils peuvent retirer leur consentement en tout temps et leur expliquez les conséquences de ce retrait.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vous tenez compte des attentes raisonnables de la personne lorsque vous cherchez à déterminer la façon d'obtenir le consentement; par exemple, le consentement positif et explicite est nécessaire si l'information est sensible.

  ☐ Oui ☐ Non

- Vous réexaminez périodiquement les dossiers de chaque personne relativement au consentement et au retrait du consentement et vous les tenez à jour.

  ☐ Oui ☐ Non

- Vous prenez note du mécanisme qui a été utilisé pour obtenir le consentement (par ex. au téléphone, par écrit, par courriel, etc.).

  ☐ Oui ☐ Non

- Vous vérifiez quand et pour quelles raisons le consentement pour la collecte de renseignements personnels n'a pu être obtenu d'une personne.

  ☐ Oui ☐ Non

- Vous évaluez les démarches entreprises par votre personnel pour obtenir le consentement d'un client et lui montrez les options qui s'offrent à lui.

  ☐ Oui ☐ Non

- Vous réévaluez régulièrement le processus utilisé pour obtenir le consentement d'un client.

  ☐ Oui ☐ Non

- Vous avez mis en place une procédure afin de veiller à ce que le consentement soit accordé avant que les renseignements personnels ne soient divulgués au sein ou à l'extérieur de votre organisation.

  ☐ Oui ☐ Non

Principe 4 La limitation de la collecte

La collecte de renseignements personnels doit se limiter à ce qui est nécessaire dans le cadre des objectifs que s'est fixés l'organisation. On doit utiliser des moyens justes et légaux pour recueillir l'information.

Objectifs

Ce principe limite la quantité et le type de renseignements personnels que vous pouvez recueillir de quelque source que ce soit, y compris des tierces parties.

Vous devez être en mesure d'établir un lien clair entre l'information que vous recueillez et les objectifs que vous vous êtes fixés pour la collecte d'information. Selon ce principe, vous ne devez pas amasser des renseignements personnels qui ne sont pas nécessaires à la poursuite des objectifs fixés.

Risque potentiel

- Le fait de ne pas limiter la collecte de renseignements personnels augmente la quantité de données dont vous devez assurer la gestion et peut entraîner des frais additionnels pour votre organisation ainsi que plus de responsabilités.
- Plus vous recueillez d'information, plus vous risquez de commettre des erreurs.
- Une collecte injustifiée ou illégale peut vous exposer à des accusations de pratiques commerciales malhonnêtes.
- En recueillant plus d'information qu'il n'est nécessaire pour atteindre vos objectifs, vous risquez d'importuner vos clients et ainsi de perdre des contrats.
- Si votre organisation recueille de l'information par des moyens électroniques par ex. des fichiers de témoins (cookies), le fait de ne pas informer vos clients pourrait entraîner des réactions défavorables vis-à-vis votre organisation.

Mise en application du principe

Ce que vous devez faire

- Vous limitez à la fois le type et la quantité de renseignements personnels que vous recueillez uniquement à ce qui est nécessaire pour atteindre le ou les objectif(s) fixé(s).

  ☐ Oui ☐ Non

- Vous recueillez les renseignements personnels de façon juste et légale et vous ne trompez pas les personnes et ne les induisez pas en erreur.

  ☐ Oui ☐ Non

- Vous ne recueillez pas de renseignements personnels à tort et à travers.

  ☐ Oui ☐ Non

- Vous décrivez quel type de renseignements personnels vous recueillez et la façon dont ils seront utilisés et divulgués.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vous définissez clairement vos méthodes de collecte de renseignements personnels en évitant les formulations subjectives ou ambiguës qui peuvent créer de la confusion chez les clients.

  ☐ Oui ☐ Non

- Vous limitez la quantité et le type d'information que vous recueillez à ce à quoi la personne avait accordé son consentement.

  ☐ Oui ☐ Non

- Vous informez les clients des options qui leur sont offertes de limiter la collecte de leurs renseignements personnels, lorsque de telles options existent.

  ☐ Oui ☐ Non

- Vous sollicitez ou avez obtenu les commentaires des clients relativement à la clarté de vos méthodes de collecte et leur avez demandé s'ils les comprenaient.

  ☐ Oui ☐ Non

- Vous procédez régulièrement à l'examen du processus de collecte de l'information et des méthodes de gestion afin qu'ils soient conformes au principe visant à limiter la collecte.

  ☐ Oui ☐ Non

- Si vous recueillez des renseignements personnels d'un tiers, vous vous assurez que ce dernier a obtenu le consentement de son client pour les divulguer.

  ☐ Oui ☐ Non

- Votre organisation utilise le consentement volontaire avant de se servir de « cookies » ou de toute autre information obtenue par un moyen électronique.

  ☐ Oui ☐ Non

Principe 5 La limitation de l'utilisation, de la communication et de la conservation

Les renseignements personnels ne devront pas être utilisés ni divulgués pour des motifs autres que ceux pour lesquels ils avaient été recueillis, sauf si l'on a obtenu le consentement éclairé de la personne ou si la loi l'exige. Les renseignements personnels ne seront conservés que le temps nécessaire pour atteindre les objectifs fixés.

Objectifs

Vous devriez utiliser ou divulguer les renseignements personnels uniquement aux fins décrites à la personne au moment de la collecte. Des utilisations ou divulgations autres que celles déjà convenues ne sont permises qu'avec le consentement de la personne ou si la loi l'exige.

Ce principe vous impose la responsabilité de conserver les renseignements personnels pour une durée limitée; soit celle qui est spécifiée par les normes de l'industrie ou par la législation applicable ou seulement aussi longtemps qu'il est nécessaire pour atteindre les objectifs fixés.

Risque potentiel

- Le fait d'utiliser ou de divulguer des renseignements personnels pour des motifs autres que ceux qui ont été déclarés peut miner la confiance du client et entraîner des accusations de pratiques commerciales trompeuses.

- Si vous n'avez pas de calendrier précis quant à la conservation de l'information, vous courez le risque, soit de conserver l'information trop longtemps et ainsi d'entraîner des frais de gestion supplémentaires, soit de détruire l'information trop tôt, compromettant ainsi l'accès des particuliers aux renseignements les concernant et compromettant l'usage que vous pourriez faire d'une information utile.

Mise en application du principe

Ce que vous devez faire

- Vous utilisez et divulguez les renseignements personnels qui sont sous votre contrôle seulement dans le but qui a été fixé pour justifier la collecte, à moins que vous n'ayez obtenu un consentement ou que l'utilisation ou la divulgation ne soit exigée par la loi.

  ☐ Oui ☐ Non

- Vous notez l'utilisation que vous faites des renseignements personnels pour un but autre que celui qui avait été indiqué aux clients lorsque vous avez obtenu leur consentement.

  ☐ Oui ☐ Non

- Vous conservez l'information le temps qui est nécessaire pour atteindre les objectifs fixés (vous avez comme politique de détruire les renseignements personnels de vos bases de données).

  ☐ Oui ☐ Non

- Vous conservez les renseignements personnels utilisés pour prendre une décision au sujet d'une personne assez longtemps pour permettre à la personne d'avoir accès aux données et d'en vérifier l'exactitude.

  ☐ Oui ☐ Non

- Vous avez établi des procédures visant à assurer la destruction sécuritaire des renseignements personnels.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vous utilisez et divulguez les renseignements personnels seulement aux fins qui avaient été déterminées au moment de la collecte.

  ☐ Oui ☐ Non

- Vous avez déterminé des cas d'exception restreints et précis en ce qui concerne l'utilisation ou la communication de l'information pour des raisons autres que celles indiquées au moment de la collecte.

  ☐ Oui ☐ Non

- Vous avez établi tant des politiques que des restrictions techniques afin de limiter l'utilisation et la divulgation des renseignements personnels aux objectifs que vous avez fixés.

  ☐ Oui ☐ Non

- Vous avisez tout le personnel concerné des restrictions relatives à l'utilisation et à la divulgation des renseignements personnels.

  ☐ Oui ☐ Non

- Vous assurez régulièrement le suivi de vos procédures, contrats légaux, politiques et contrôles techniques afin de veiller à ce que les restrictions pertinentes sur l'utilisation et la divulgation des renseignements personnels soient bien en place.

  ☐ Oui ☐ Non

- Vous transmettez des renseignements personnels à des tiers uniquement aux fins indiquées au moment de la collecte.

  ☐ Oui ☐ Non

- Vos méthodes de rétention de données comprennent des procédures précises de conservation ainsi que des durées de conservation minimum et maximum.

  ☐ Oui ☐ Non

- Vous avez établi un calendrier qui indique clairement combien de temps conserver les renseignements personnels et quand en disposer.

  ☐ Oui ☐ Non

- Vous faites connaître vos pratiques relatives à l'utilisation, à la divulgation et à la conservation de l'information aux secteurs de l'entreprise qui sont responsables de la conservation des renseignements personnels.

  ☐ Oui ☐ Non

- Vous conservez les renseignements personnels uniquement pour les motifs pour lesquels vous les avez recueillis, sauf lorsque la loi l'exige.

  ☐ Oui ☐ Non

- Les renseignements personnels qui ne sont plus nécessaires à la poursuite des objectifs fixés sont détruits, effacés ou rendus anonymes.

  ☐ Oui ☐ Non

- Vous informez les gens au sujet de vos durées de conservation et de ce que vous avez l'intention de faire avec l'information lorsque la période maximum de conservation prendra fin.

  ☐ Oui ☐ Non

- Vous mettez les renseignements personnels à jour seulement lorsque cela est pertinent.

  ☐ Oui ☐ Non

Principe 6 L'exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que nécessaire compte tenu des objectifs pour lesquels ils seront utilisés.

Objectifs

Les besoins de votre entreprise en matière d'exactitude des renseignements personnels varieront en fonction des objectifs pour lesquels vous les recueillez, les utilisez et les divulguez.

Règle générale, si vous utilisez ou divulguez des renseignements personnels sur une base de permanence, vous devriez vous assurer qu'ils soient exacts. Cependant, pour certains objectifs il ne sera pas nécessaire que l'information soit courante et à jour; dans ces cas, vous devriez vous en tenir uniquement à la mise à jour des renseignements personnels dont vous avez besoin.

Lorsque vous cherchez à déterminer le degré nécessaire d'exactitude, d'intégralité et d'actualité des données, vous devez tenir compte des exigences des objectifs que vous avez fixés et vous demander si l'utilisation ou la divulgation d'information **inexacte** pourrait causer du tort à la personne concernée.

Risque potentiel

- Le fait d'utiliser de l'information inexacte pour prendre une décision à propos de clients peut vous faire perdre des profits et une part du marché.
- Des renseignements inexacts peuvent causer du tort au client et compromettre les relations clientèle.
- Le fait de ne pas relever l'information qui est inexacte peut avoir pour conséquence que des décisions seront prises sur la base de renseignements imparfaits et peut-être même trompeurs.
- Le fait de ne pas définir les besoins précis en termes d'information courante et à jour peut entraîner des mises à jour inutiles et par le fait même gaspiller des ressources et importuner les clients.

Mise en application du principe

Ce que vous devez faire

- Vous gardez les renseignements personnels qui sont sous votre contrôle aussi exacts, complets et à jour que nécessaire compte tenu des objectifs fixés.

  ☐ Oui ☐ Non

- Vous tenez compte des intérêts des individus lorsque vous déterminez dans quelle mesure les renseignements personnels sous votre contrôle doivent être exacts, complets et à jour.

  ☐ Oui ☐ Non

- Vous veillez à ce que l'information personnelle soit suffisamment exacte afin de minimiser les risques que des données inappropriées ne soient utilisées lorsque des décisions sont prises concernant des personnes.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vos méthodes définissent quand les mises à jour sont appropriées compte tenu de vos objectifs et des intérêts de vos clients.

  ☐ Oui ☐ Non

- Vous définissez clairement toute restriction quant aux exigences en matière d'exactitude.

  ☐ Oui ☐ Non

- Vous avez des procédures pour vérifier et rectifier les renseignements personnels.

  ☐ Oui ☐ Non

- Vous informez les gens de la façon dont ils peuvent avoir accès aux renseignements personnels que vous détenez et comment ils peuvent les rectifier.

  ☐ Oui ☐ Non

- Vous évaluez périodiquement l'exactitude des renseignements de vos bases de données.

  ☐ Oui ☐ Non

Principe 7 Les mesures de sécurité

Les renseignements personnels doivent être protégés par des mesures de sécurité adaptées au niveau de sensibilité de l'information.

Objectifs

Vos mesures de sécurité, tant électroniques que physiques, devraient être adaptées et proportionnelles au niveau de sensibilité des renseignements personnels concernés. Plus le niveau de sensibilité est élevé, plus il faut protéger l'information.

Alors que certains types de renseignements personnels (par ex. des données médicales ou financières) sont généralement considérés comme sensibles, d'autres types d'information peuvent se révéler sensibles, tout dépendant du contexte.

Lorsque vous établissez le niveau de sensibilité, tenez compte de la quantité de renseignements personnels qui pourraient être révélés si des parties non autorisées les consultaient. Tenez compte également du tort qui pourrait potentiellement être causé à la personne si les données étaient mal utilisées ou divulguées sans autorisation. Plus le tort potentiel est grand, plus les exigences en matière de sécurité devraient être élevées.

Risque potentiel

- Si vous n'avez pas de mesures de sécurité appropriées, des personnes non autorisées (tant à l'intérieur qu'à l'extérieur de votre entreprise) peuvent être en mesure de consulter, d'utiliser, de copier, de divulguer, de modifier et de détruire les renseignements personnels dont vous avez la garde et que vous avez la responsabilité de protéger. De tels gestes pourraient causer des torts importants à la personne concernée par ces données et votre entreprise pourrait potentiellement en être tenue responsable.

- Si vous n'avez pas de mécanismes appropriés de contrôle d'accès, des personnes non autorisées peuvent avoir accès aux renseignements personnels et les utiliser à des fins non autorisées.

- Si vous n'avez pas de système de vérification approprié relativement à l'accès aux renseignements personnels, il est possible que les brèches de sécurité ne soit pas décelées ni réparées.

Mise en application du principe

Ce que vous devez faire

- Vous établissez des mesures de sécurité pour protéger les renseignements personnels dont vous avez la garde contre la perte ou le vol ainsi que contre l'accès, la divulgation, la duplication, l'utilisation ou la modification non autorisés.

  ☐ Oui ☐ Non

- Vos mesures de sécurité sont adaptées et proportionnelles au niveau de sensibilité des renseignements personnels dont vous avez la garde.

  ☐ Oui ☐ Non

- Vous protégez tout renseignement personnel se trouvant sous votre contrôle sans égard à son format.

  ☐ Oui ☐ Non

- Vous sensibilisez votre personnel à l'importance de protéger la confidentialité des renseignements personnels qui sont sous votre contrôle.

  ☐ Oui ☐ Non

- Vous vous départissez des renseignements personnels ou les détruisez de façon à éviter que des personnes non autorisées n'y aient accès.

  ☐ Oui ☐ Non

Pratiques exemplaires

- L'aménagement de vos locaux permet aux renseignements sur les clients et les employés de demeurer privés et confidentiels.

  ☐ Oui ☐ Non

- Une tierce partie contrôle et vérifie les systèmes de sécurité sur une base régulière.

  ☐ Oui ☐ Non

- Vous mettez tout le personnel concerné au courant de vos mesures de sécurité relativement à l'accès aux renseignements personnels, à leur utilisation, à leur divulgation et à leur destruction.

  ☐ Oui ☐ Non

- Vous prenez note des utilisations fautives de renseignements personnels et en avisez les clients concernés.

  ☐ Oui ☐ Non

- Vous avez une politique de sécurité des renseignements qui comprend des exigences précises quant au processus d'identification et d'autorisation du personnel ayant accès aux renseignements personnels.

  ☐ Oui ☐ Non

- Chaque membre du personnel a un identificateur unique utilisé pour avoir accès aux renseignements personnels.

  ☐ Oui ☐ Non

- Chaque membre du personnel est authentifié (par exemple par l'utilisation d'un mot de passe) afin d'avoir accès aux renseignements personnels, et ce, à l'aide d'un mécanisme d'authentification correspondant à la portée de l'accès et à la sensibilité de l'information.

  ☐ Oui ☐ Non

- Vous avez une politique de sécurité de l'information qui comprend des exigences précises visant à assurer la confidentialité des renseignements personnels.

  ☐ Oui ☐ Non

- Vous transmettez les renseignements personnels par voie de communication protégée et (ou) vous chiffrez toutes transmissions par voie ouverte.

  ☐ Oui ☐ Non

- Vous assurez la sécurité des documents sur papier qui contiennent des renseignements personnels.

  ☐ Oui ☐ Non

- Vous avez une politique de sécurité de l'information qui comprend des exigences précises visant la création de pistes de vérification pour tout système d'information traitant des renseignements personnels ainsi que pour la surveillance active de tous ces systèmes.

  ☐ Oui ☐ Non

- Des systèmes anti-intrusion (gérés par le système central ou le réseau) sont mis en place pour tous les systèmes d'information contenant des renseignements personnels.

  ☐ Oui ☐ Non

- Des procédures ont été définies pour contrôler les systèmes anti-intrusion et répondre aux alertes qui surviennent.

  ☐ Oui ☐ Non

Principe 8 La transparence

Une organisation doit communiquer rapidement aux particuliers l'information précise sur ses politiques et pratiques en matière de gestion des renseignements personnels.

Objectifs

Ce principe vous met dans l'obligation de faire preuve d'ouverture et de transparence dans vos méthodes de gestion de l'information. Ainsi, ce principe veille à ce que votre responsabilité vis-à-vis les renseignements personnels soit efficacement établie et que les personnes puissent obtenir l'information dont elles ont besoin afin de prendre des décisions éclairées relativement à leur relation d'affaires avec vous. L'ouverture et la transparence sont des composantes essentielles de la confiance du client.

L'information que vous transmettez sur vos politiques et vos pratiques doit comprendre le nom (ou le titre) et l'adresse de la personne qui en est responsable et à qui les particuliers peuvent acheminer plaintes et requêtes.

De plus, vous devez décrire clairement :

- comment les personnes peuvent avoir accès aux renseignements personnels dont vous avez le contrôle;
- le type de renseignements personnels que vous détenez;
- comment vous utilisez les renseignements personnels; et
- quels renseignements personnels vous communiquez à des organisations apparentées.

Enfin, vous devez rendre accessible au public un exemplaire de tout dépliant ou de tout autre document informatif qui explique vos politiques, pratiques, normes et codes en matière de gestion de la confidentialité et de l'information.

Risque potentiel

- Lorsque le programme de protection de la vie privée d'une organisation n'est pas accessible, cela empêche les gens de comprendre comment celle-ci gère et protège leurs renseignements personnels et cela peut réduire les chances qu'a une organisation d'obtenir un consentement éclairé.
- Sans transparence, vous sacrifiez la confiance des clients et minez la gestion des relations avec vos clients.

Mise en application du principe

Ce que vous devez faire

- Vous faites preuve de transparence en ce qui a trait à vos politiques et pratiques en matière de gestion des renseignements personnels.

  ☐ Oui ☐ Non

- Vous communiquez des détails sur le type de renseignements personnels que vous détenez, sur la façon dont vous les utilisez, les divulguez et dont on peut y avoir accès.

  ☐ Oui ☐ Non

- Vous permettez aux particuliers d'obtenir de l'information sur vos politiques et pratiques sans qu'ils aient à déployer trop d'efforts.

  ☐ Oui ☐ Non

- Vous communiquez cette information sous une forme que tous peuvent comprendre.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vous rendez accessible l'information sur vos politiques et pratiques d'une variété de façons, tout dépendant de la nature de votre entreprise (par ex. au moyen de dépliants, d'accès en direct ou de ligne téléphonique sans frais).

  ☐ Oui ☐ Non

- Une description de votre programme de protection des renseignements personnels est incluse dans tous les accords et les contrats conclus avec des tiers.

  ☐ Oui ☐ Non

- Vous expliquez l'utilisation de tout outil de repérage non visible tel que les données sur le parcours et les GIF transparents (Web Bug).

  ☐ Oui ☐ Non

- Vos employés comprennent le programme de protection des renseignements personnels de votre organisation et s'engagent à s'y conformer.

  ☐ Oui ☐ Non

- Vous montrez à votre personnel que vous respectez vos politiques et pratiques en matière de protection des renseignements personnels par l'entremise de moyens appropriés (par ex. affiliations professionnelles, sceaux de confidentialité, publication d'avis de non-conformité).

  ☐ Oui ☐ Non

Principe 9 L'accès aux renseignements personnels

Sur demande, toute personne doit être informée de l'existence, de l'utilisation et de la divulgation de renseignements qui la concernent et on devra lui donner accès à cette information. On devra permettre à chacun de contester l'exactitude et l'intégralité de l'information et de la modifier au besoin.

Objectifs

Afin que les personnes puissent prendre des décisions éclairées dans le cadre de leur relation d'affaires avec vous et qu'elles puissent exercer de façon efficace un certain contrôle sur leurs renseignements personnels, elles doivent pouvoir avoir accès à ces derniers. Il est tout aussi important qu'elles puissent également rectifier de l'information qui se révèle inexacte ou incomplète.

Il se peut qu'il ne soit pas toujours approprié ou possible pour vous d'offrir l'accès à tous les renseignements personnels que vous détenez. Néanmoins, vous avez la responsabilité de rendre les renseignements aussi accessibles que possible. Les raisons que vous évoquez pour refuser à une personne l'accès aux renseignements la concernant devraient être restreintes, précises, vraisemblables et justifiées. Lorsque vous ne pouvez pas offrir un accès complet, vous devriez en fournir une explication à la personne.

Ce principe vous rend responsable de mettre en valeur le droit qu'a toute personne de consulter et de rectifier l'information sur demande.

Risque potentiel

- Le fait de ne pas offrir l'accès à l'information aux clients peut donner lieu à des données inexactes.
- Le fait de ne pas prendre en compte l'accès client dans la conception des systèmes de gestion de l'information peut entraîner ultérieurement des frais importants.
- Le fait de ne pas tenir compte du droit du client de mettre en doute la conformité de votre organisation aux principes aggravera les plaintes relatives à la protection des renseignements personnels; il en coûtera ainsi beaucoup plus pour résoudre les conflits.

Mise en application du principe

Ce que vous devez faire

- À leur demande, vous dites aux gens si vous détenez des renseignements personnels à leur sujet et leur donnez accès à ces données, sauf dans certains cas précis.

  ☐ Oui ☐ Non

- Vous dites aux gens comment leurs renseignements personnels sont utilisés et à qui ils ont été divulgués.

  ☐ Oui ☐ Non

- Vous donnez suite à la demande d'un particulier qui désire avoir accès à l'information, et ce, dans des délais raisonnables et à des frais minimes ou de préférence, gratuitement.

  ☐ Oui ☐ Non

- Vous fournissez l'information demandée à la personne sous une forme qui est en général intelligible ainsi que toute explication nécessaire pour l'aider à la saisir.

  ☐ Oui ☐ Non

- Vous permettez à la personne de contester l'exactitude et l'intégralité des renseignements personnels qui sont sous votre contrôle et les modifiez au besoin.

  ☐ Oui ☐ Non

- Vous joignez une mention de désaccord aux dossiers si vous ne pouvez pas approuver la modification demandée.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Vous authentifiez l'identité de la personne qui fait une demande de renseignements personnels.

  ☐ Oui ☐ Non

- Vous fournissez aux particuliers une liste des organisations auxquelles vous avez peut-être divulgué leurs renseignements personnels si vous ne pouvez pas leur donner une liste des informations qui ont réellement été transmises.

  ☐ Oui ☐ Non

- Vous envoyez les données corrigées, ou la mention de désaccord, aux tierces parties qui ont eu accès aux renseignements personnels en question, selon ce qui convient.

  ☐ Oui ☐ Non

Principe 10 Plainte contre le non-respect des principes

Toute personne doit pouvoir porter plainte contre le non-respect des principes énoncés ci-dessus auprès de la personne ou des personnes à qui incombe la responsabilité de veiller à ce que l'organisation s'y conforme.

Objectifs

Ce principe porte sur le droit de chacun de mettre en doute votre conformité à ces principes de protection des renseignements personnels et aux politiques et pratiques en matière de confidentialité que vous avez énoncées. Il vous confie la responsabilité de permettre à chacun d'exercer de façon efficace ce droit. L'objectif n'est pas seulement d'améliorer votre responsabilité mais également d'habiliter la personne.

Risque potentiel

- S'il n'existe aucun processus efficace pour porter plainte contre le non-respect des principes énoncés, les particuliers ne pourront pas évaluer votre programme de protection de la vie privée ainsi que votre façon de traiter les renseignements personnels à leur sujet.
- Le fait de ne pas offrir cette composante du service à la clientèle pourrait entraîner de l'insatisfaction chez le client et la perte de contrats.
- Si vous n'avez aucun processus efficace pour porter plainte contre le non-respect des principes énoncés, vous risquez de perdre des possibilités d'améliorer les pratiques de votre entreprise.

Mise en application du principe

Ce que vous devez faire

- Vous avez établi des procédures pour recevoir des plaintes et des requêtes relatives à votre façon de gérer les renseignements personnels et y répondre.

  ☐ Oui ☐ Non

- Vous expliquez vos procédures en matière de requête et de plaintes aux particuliers.

  ☐ Oui ☐ Non

- Vous étudiez toutes les plaintes.

  ☐ Oui ☐ Non

- Vous prenez les mesures nécessaires pour rectifier la situation si vous considérez qu'une plainte est justifiée.

  ☐ Oui ☐ Non

- Vous modifiez vos politiques et pratiques de gestion de l'information au besoin.

  ☐ Oui ☐ Non

Pratiques exemplaires

- Votre procédé de vérification du respect des principes énoncés est facilement accessible et convivial.

  ☐ Oui ☐ Non

- Votre personnel répond aux demandes du public de manière équitable, exacte et rapide.

  ☐ Oui ☐ Non

- Les processus de résolution de plainte et de conflit sont régulièrement contrôlés pour en évaluer l'efficacité, l'équité, l'impartialité, la confidentialité, la convivialité et la rapidité.

  ☐ Oui ☐ Non

Glossaire des termes

Consentement

Il doit y avoir consentement délibéré pour que des données sur des renseignements personnels soient recueillies, utilisées et divulguées. Ce consentement peut être soit explicite ou implicite et devrait comprendre une explication concernant les conséquences du retrait du consentement.

Le consentement explicite est donné sans ambiguïté, soit verbalement ou par écrit. Il est sans équivoque et n'exige aucune inférence de la part de l'organisation qui veut l'obtenir.

Le consentement implicite est donné lorsque l'action ou l'inaction d'une personne le laissent entendre suffisamment.

Le consentement ne devrait jamais être conditionnel à ce qu'un produit ou un service ne soit fourni, sauf si l'information demandée est nécessaire pour atteindre un objectif légitime qui a été clairement défini.

Définition des objectifs

Les objectifs, qui comprennent la raison pour laquelle l'information a été recueillie et comment elle est utilisée, doivent être fixés par l'organisation au moment de la collecte des renseignements ou avant.

Le motif de la collecte de renseignements devrait être documenté. On devrait informer la personne de qui on obtient l'information pourquoi on exige ces renseignements.

Divulgation

Il y a divulgation de renseignements lorsque l'information personnelle est rendue accessible à d'autres secteurs d'une même organisation pour lesquels l'information n'avait pas été amassée au préalable ou à d'autres à l'extérieur de l'organisation.

Droit d'accès (accès des particuliers)

Si elle en fait la demande, toute personne doit être informée de l'existence, de l'utilisation et de la divulgation de renseignements personnels la concernant et pourra avoir accès à cette information.

Toute personne doit avoir le droit de contester l'exactitude et l'intégralité de l'information et de la faire modifier tel que nécessaire.

Durée de conservation

La durée de conservation est le temps que les renseignements personnels sont gardés. L'information personnelle ne devrait pas être conservée plus longtemps qu'il n'est nécessaire pour atteindre les objectifs pour lesquels elle a été recueillie; elle doit toutefois être conservée assez longtemps pour permettre aux personnes d'y avoir accès si elle a constitué la base d'une décision qui les concerne.

Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que nécessaire pour atteindre les objectifs pour lesquels ils sont recueillis. Les renseignements personnels seront mis à jour uniquement lorsque cela sera nécessaire à la poursuite des objectifs pour lesquels ils ont été recueillis.

Information identifiable personnelle

Une information personnelle identifiable est toute donnée qui lie de façon unique une personne à d'autres ensembles de données. Il s'agit par exemple des NIP (numéros d'identification personnels), des cartes d'accès, des mots de passe, des lectures d'empreintes rétiniennes et digitales, des courriels et des adresses Internet. Ce type d'information devrait être traité de la même manière que les renseignements personnels qui ne sont pas recueillis en ligne.

Limitation de la collecte

La collecte de renseignements personnels doit se limiter à ce qui est nécessaire à la poursuite des objectifs fixés par l'organisation.

L'information doit être recueillie par des moyens justes et légaux. Le type et la quantité de renseignements amassés devraient se limiter à ce qui est nécessaire dans le cadre des objectifs fixés. Les membres du personnel doivent être en mesure d'expliquer le motif de la collecte de renseignements.

Limitation de l'utilisation, de la divulgation et de la durée de conservation

Les renseignements personnels ne doivent pas être utilisés ni communiqués à des fins autres que celles pour lesquelles ils ont été recueillis, sauf si l'on a obtenu le consentement de la personne ou si la loi l'exige.

Toute nouvelle utilisation des renseignements personnels doit être signifiée. On doit obtenir le consentement de la personne avant d'utiliser l'information à cette nouvelle fin.

Les renseignements personnels ne devraient être conservés que le temps nécessaire pour atteindre les objectifs fixés. Il faudrait instituer des durées de conservation maximum et minimum qui tiennent compte de toutes exigences et restrictions légales et de tous mécanismes de recours.

On doit se défaire d'une information qui n'a pas de but précis ou qui ne convient plus à l'objectif fixé, et ce, d'une manière qui préviendra l'accès illégitime, comme au moyen du déchiquetage des documents papiers ou de la suppression des fichiers électroniques.

On devrait établir des politiques décrivant le type de mises à jour de l'information et leur fréquence.

Mesures de sécurité

Les renseignements personnels doivent être protégés par des mesures de sécurité adaptées à la sensibilité de l'information.

Plainte contre le non-respect des principes énoncés

Toute personne doit pouvoir contester le non-respect des principes énoncés auprès de la ou des personnes responsables de veiller à ce que l'organisation s'y conforme.

Protection de la vie privée

La protection de la vie privée est le droit fondamental de chacun de décider du traitement de ses données personnelles ainsi que de protéger sa sphère intime. Les violations de la vie privée comprennent :

- l'acquisition illégitime de renseignements personnels y compris leur consultation, leur collecte et leur distribution;
- l'usage abusif de l'information y compris son utilisation pour des raisons autres que celles pour lesquelles elle a été expressément recueillie ou son transfert à des tiers;
- la sollicitation non désirée de données personnelles; et
- le stockage inadéquat de l'information.

Renseignement personnel

Un renseignement personnel est toute information factuelle ou subjective, enregistrée ou non, concernant une personne identifiable. Il s'agit par exemple du nom, de l'âge, des numéros d'identification, du revenu, de l'origine ethnique, du groupe sanguin, des opinions, des évaluations, des commentaires, du statut social, des mesures disciplinaires, des dossiers d'employé, des dossiers de crédit ou de prêt, des dossiers médicaux ou de l'existence d'un conflit entre un client et un commerçant.

Responsabilité

Une organisation est responsable de l'information se trouvant sous son contrôle et désignera une ou des personnes qui devront s'assurer qu'elle respecte les principes de pratiques équitables de traitement de l'information ainsi que la législation pertinente.

Transparence Une organisation doit faire en sorte que l'information touchant précisément ses politiques et ses pratiques en matière de gestion des renseignements personnels soit disponible rapidement et sous une forme intelligible. Les clients, les usagers et les employés doivent être informés de ces politiques.

Utilisation L'utilisation a trait au traitement et à la gestion des renseignements personnels au sein d'une organisation.

Liens vers d'autres sites sur la confidentialité

Pour obtenir plus de renseignements et de ressources sur la protection de la vie privée et sur des sujets connexes, consultez la liste suivante de sites Web. Ces sites constituent un échantillon de perspectives internationales et comprennent d'autres liens à une mine de renseignements sur la protection de la vie privée.

- **Le Bureau du commissaire à l'information et à la protection de la vie privée/Ontario**
  www.ipc.on.ca

- **Commission d'accès à l'information du Québec**
  www.cai.gouv.qc.ca

- **Commissaire à la protection de la vie privée du Canada**
  www.privcom.gc.ca

- **Federal Trade Commission (États-Unis d'Amérique)**
  www.ftc.gov

- **International Virtual Privacy Office**
  www.privacyservice.org

- **OCDE – Sécurité de l'information et protection de la vie privée**
  www.oecd.org/FR/home/0,,FR-home-43-nodirectorate-no-no-no-29,00.html

- **Australian Privacy Commissioner**
  www.privacy.gov.au